ITSY 2442 - Incident Response & Handling 401 Course Syllabus

Description
In-depth coverage of incident response and incident handling, including identifying sources of attacks and security breaches; analyzing security logs; recovering the system to normal; performing postmortem analysis; and implementing and modifying security measures.
Prerequisites ITSY 1400
Credits 4
Lecture Hours 3
Lab Hours 3
Extended Hours 0
Contact Hours 96
State Approval Code 11.1003
Instructor Name Erik Choron
Semester/Year Fall 2024

Meeting Time and Location
Online—students are expected to spend at least 3-4 hours per week reading, reviewing, and participating in assigned activities for successful completion of this course.

Alternate Operations During Campus Closure
In the event of an emergency or announced campus closure due to a natural disaster or pandemic, it may be necessary for Panola College to move to altered operations. During this time, Panola College may opt to continue delivery of instruction through methods that include, but are not limited to: online learning management system (CANVAS), online conferencing, email messaging, and/or an alternate schedule. It is the responsibility of the student to monitor Panola College's website (www.panola.edu) for instructions about continuing courses remotely, CANVAS for each class for course-specific communication, and Panola College email for important general information.

Student Basic Needs
Unexpected circumstances may arise, but Panola College offers various resources to support students. If you need mental health services or are facing challenges with transportation, affording class materials and supplies, or accessing food regularly—issues that may impact your class performance—please visit panola.edu/resources.

Class Attendance
Regular and punctual attendance of classes and laboratories is required of all students. When a student has been ill or absent from class for approved extracurricular activities, he or she should be allowed, as far as possible, to make up for the missed work. If a student has not actively participated by the census date, they will be dropped by the instructor for non-attendance. This policy applies to courses that are in-person, online, hybrid, and hyflex.

Attendance in online courses is determined by submission of an assignment or participation in an activity. According to federal guidelines, simply logging into a distance learning course without participating in an academic assignment does not constitute attendance. Distance learning is defined as when a majority (more than 50%) of instruction occurs when the instructor and students are in separate physical locations. Students must engage in an academic activity prior to the course census date.

When an instructor feels that a student has been absent to such a degree as to invalidate the learning experience, the instructor may recommend to the Vice President of Instruction that the student be withdrawn from the course. Instructors may seek to withdraw students for non-attendance after they have accumulated the following number of absences:

Fall or spring semesters:

3 or more class meeting times per week - 5 absences

2 class meeting times per week - 3 absences

1 class meeting per week - 2 absences

The student is responsible for seeing that he or she has been officially withdrawn from a class. A student who stops attendance in a class without officially withdrawing from that class will be given a failing grade; consequently, the student must follow official withdrawal procedures in the Admissions/Records Office.

Please note: Health Science and Cosmetology courses may require more stringent attendance policies based on their accreditation agencies. Please see the addendum and/or program handbook for further information concerning attendance.

Pregnant/Parenting Policy

Panola College welcomes pregnant and parenting students as a part of the student body. This institution is committed to providing support and adaptations for a successful educational experience for pregnant and parenting students. Students experiencing a need for accommodations related to pregnancy or parenting will find a Pregnancy and Parenting Accommodations Request form in the Student Handbook or may request the form from the course instructor.

Artificial Intelligence (AI) Course Policy

No use of Generative AI permitted.

This option assumes that all work submitted by students will be generated by the students themselves, whether they are working individually or in groups. Students should not have another person or entity do the writing of any portion of an assignment, which includes hiring a person or a company to write assignments and/or using artificial intelligence (AI) tools like ChatGPT. Use of any AI-generated content in this course qualifies as academic dishonesty and violates Panola College's standards of academic integrity.

Student Learning Outcomes

Critical Thinking Skills – to include creative thinking, innovation, inquiry and analysis, evaluation and syntheses of information

- CT1: Generate and communicate ideas by combining, changing, or reapplying existing information
- CT2: Gather and assess information relevant to a question
- CT3: Analyze, evaluate, and synthesize information

Communication Skills – to include effective development, interpretation, and expression of ideas through written, oral, and visual communication

- CS1: Develop, interpret, and express ideas through written communication
- CS2: Develop, interpret, and express ideas through oral communication
- CS3: Develop, interpret, and express ideas through visual communication

Empirical and Quantitative Skills – to include the manipulation and analysis of numerical data or observable facts resulting in informed conclusions

- EQS1: Manipulate and analyze numerical data and arrive at an informed conclusion
- EQS2: Manipulate and analyze observable facts and arrive at an informed conclusion

Personal Responsibility – to include the ability to connect choices, actions, and consequences to ethical decision-making

- PR1: Evaluate choices and actions and relate consequences to decision-making

Social Responsibility – to include intercultural competence, knowledge of civic responsibility, and the ability to engage effectively in regional, national, and global communities

- SR1: Demonstrate intercultural competence
- SR2: Identify civic responsibility

Instructional Goals and Purposes

The purpose of this course is to teach students and expand on basic security fundamentals relevant to the information security and information assurance management practices within the workforce. The student will be asked to identify best practices within information technology security concerns and be introduced to national standards of practice.

Learning Outcomes

1. Understand the need for incident response and handling
2. Be able to explain the usage of basic security mechanisms and controls
3. Be proficient in using popular tools required by information security professionals
4. Be prepared for the CompTIA Security+ exam

Specific Course Objectives (includes SCANS)

After studying all materials and resources presented in the course, the student will be able to:

1. **Incident Response**
    1. Incident Response Overview
    2. Identifying the Investigative Lead
    3. Identifying the People and Systems Involved
2. **Incident Response Data and Tools**
    1. Workstation Data Investigation
    2. Network Data Investigation
    3. Commonly Used Tools for Auditing
    4. System Event Logs
3. **Chain of Custody**
    1. Chain of Custody Overview
    2. Two Person Integrity
    3. Data or Evidence Storage
4. **Mitigation**
    1. Identifying Systems Involved
    2. Blocking the Spread of Malicious Activity
    3. Network Analysis
    4. Patching the System
5. **Recovery**
    1. System Verification
    2. Auditing and Logging of Practices
    3. Identifying the System Owner for Restoration and Authorization

Course Content

Students in all sections of this course will be required to do the following:

1. Students will complete quizzes located within each module. They may also have access to tutorial videos, practice tests and other training materials located within relevant modules.
2. Students must complete the Mid-Term and Final exams using an official testing proctor.

Methods of Instruction/Course Format/Delivery

This course is offered as an Internet class via the Canvas Learning Management System. The online learners will not meet as a traditional class but will have access to any tutorial videos, lab simulation exercises, and practice questions which may be included. Each chapter has an associated course or module assigned from supplemental material provided inside the Canvas course. All assignments should be completed by going through the assignment link in Canvas. This will ensure that the grade will be recorded in the Canvas Gradebook which is the official grade location.

The students will have access to the instructor via the Canvas Message system, posted office hours, or by scheduled appointments. If a Canvas message is not answered within 24 hours the student can email the instructor using their Panola College email address. Students can also contact the instructor via their office phone or in person during posted office hours or scheduled appointments. Students should check Canvas Announcements and Canvas Messages each day for possible updated information from the instructor.

Major Assignments/Assessments

The following items are assigned and assessed during the semester and used to calculate the student's final grade.

Assignments

Students will access assignments from their Canvas course which demonstrate mastery of the chapter concepts and skills.

Assessments

1. Module Quizzes
2. Exams
    1. Midterm
    2. Final

plus your one time syllabus quiz

Course Grade

	Each	Total
Syllabus Quiz	5	5
Quizzes (6)	20	120
Midterm Exam	105	105
Final Exam	110	110
Total		340

Final grades will be calculated based on the following:

A: 306-340
B: 272-305
C: 238-271
D: 204-237
F: <=204

Texts Materials, and Supplies

- The students are required to purchase The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) eBook ISBN: 978-1-64274-329-6
- Access to a computer with a strong Internet connection

Required Readings

- The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601) eBook ISBN: 978-1-64274-329-6 - chapters 14

Recommended Readings

None

Addendum

Should you need books for this course, please contact or go to the Dean of Career and Technical Programs' office in the Martha Miller Administration Building, Room 1300. Books are loaned out for the semester free of charge and are limited by availability.

Other

- Courses conducted via video conferencing may be recorded and shared for instructional purposes by the instructor.
- For current texts and materials, use the following link to access bookstore listings: https://www.panolacollegestore.com.
- For testing services, use the following link: https://www.panola.edu/student-services/studentsupport/academic-testing-center.
- If any student in this class has special classroom or testing needs because of a physical learning or emotional condition, please contact the ADA Student Coordinator in Support Services located in the Charles C. Matthews Student Center or go to https://www.panola.edu/studentservices/student-support/disability-support-services for more information.
- Withdrawing from a course is the student's responsibility. Students who do not attend class and who do not withdraw will receive the grade earned for the course.
- Student Handbook: https://www.panola.edu/ (located on at the bottom under student)

SCANS Criteria

1. Foundation skills are defined in three areas: basic skills, thinking skills, and personal qualities.
    a. Basic Skills: A worker must read, write, perform arithmetic and mathematical operations, listen, and speak effectively. These skills include:
        i. Reading: locate, understand, and interpret written information in prose and in documents such as manuals, graphs, and schedules.
        ii. Writing: communicate thoughts, ideas, information, and messages in writing, and create documents such as letters, directions, manuals, reports, graphs, and flow charts.
        iii. Arithmetic and Mathematical Operations: perform basic computations and approach practical problems by choosing appropriately from a variety of mathematical techniques.
        iv. Listening: receive, attend to, interpret, and respond to verbal messages and other cues.
        v. Speaking: Organize ideas and communicate orally.
    b. Thinking Skills: A worker must think creatively, make decisions, solve problems, visualize, know how to learn, and reason effectively. These skills include:
        i. Creative Thinking: generate new ideas.
        ii. Decision Making: specify goals and constraints, generate alternatives, consider risks, and evaluate and choose the best alternative.
        iii. Problem Solving: recognize problems and devise and implement plan of action.
        iv. Visualize ("Seeing Things in the Mind's Eye"): organize and process symbols, pictures, graphs, objects, and other information.
        v. Knowing How to Learn: use efficient learning techniques to acquire and apply new knowledge and skills.
        vi. Reasoning: discover a rule or principle underlying the relationship between two or more objects and apply it when solving a problem.
    c. Personal Qualities: A worker must display responsibility, self-esteem, sociability, self management, integrity, and honesty.
        i. Responsibility: exert a high level of effort and persevere toward goal attainment.
        ii. Self-Esteem: believe in one's own self-worth and maintain a positive view of oneself.
        iii. Sociability: demonstrate understanding, friendliness, adaptability, empathy, and politeness in group settings.
        iv. Self-Management: assess oneself accurately, set personal goals, monitor progress, and exhibit self-control.
        v. Integrity and Honesty: choose ethical courses of action.
2. Workplace competencies are defined in five areas: resources, interpersonal skills, information, systems, and technology.
    a. Resources: A worker must identify, organize, plan, and allocate resources effectively.

i. Time: select goal-relevant activities, rank them, allocate time, and prepare and follow schedules.
ii. Money: Use or prepare budgets, make forecasts, keep records, and make adjustments to meet objectives.
iii. Material and Facilities: Acquire, store, allocate, and use materials or space efficiently. Examples: construct a decision timeline chart; use computer software to plan a project; prepare a budget; conduct a cost/benefits analysis; design an RFP process; write a job description; develop a staffing plan.

b. Interpersonal Skills: A worker must work with others effectively.
i. Participate as a Member of a Team: contribute to group effort.
ii. Teach Others New Skills.
iii. Serve Clients/Customers: work to satisfy customer's expectations.
iv. Exercise Leadership: communicate ideas to justify position, persuade and convince others, responsibly challenge existing procedures and policies.
v. Negotiate: work toward agreements involving exchange of resources, resolve divergent interests.
vi. Work with Diversity: work well with men and women from diverse backgrounds. Examples: collaborate with a group member to solve a problem; work through a group conflict situation, train a colleague; deal with a dissatisfied customer in person; select and use appropriate leadership styles; use effective delegation techniques; conduct an individual or team negotiation; demonstrate an understanding of how people from different cultural backgrounds might behave in various situations.

c. Information: A worker must be able to acquire and use information.
i. Acquire and Evaluate Information.
ii. Organize and Maintain Information.
iii. Interpret and Communicate Information.
iv. Use Computers to Process Information. Examples: research and collect data from various sources; develop a form to collect data; develop an inventory record-keeping system; produce a report using graphics; make an oral presentation using various media; use on-line computer databases to research a report; use a computer spreadsheet to develop a budget.

d. Systems: A worker must understand complex interrelationships.
i. Understand Systems: know how social, organizational, and technological systems work and operate effectively with them.
ii. Monitor and Correct Performance: distinguish trends, predict impacts on system operations, diagnose deviations in systems' performance and correct malfunctions.
iii. Improve or Design Systems: suggest modifications to existing systems and develop new or alternative systems to improve performance. Examples: draw and interpret an organizational chart; develop a monitoring process; choose a situation needing improvement, break it down, examine it, propose an improvement, and implement it.

e. Technology: A worker must be able to work with a variety of technologies.
i. Select Technology: choose procedures, tools or equipment including computers and related technologies.
ii. Apply Technologies to Task: understand overall intent and proper procedures for setup and operation of equipment.
iii. Maintain and Troubleshoot Equipment: Prevent, identify, or solve problems with equipment, including computers and other technologies. Examples: read equipment descriptions and technical specifications to select equipment to meet needs; set up and assemble appropriate equipment from instructions; read and follow directions for troubleshooting and repairing equipment.